

**ORDER**

**DEPARTMENT OF TRANSPORTATION  
FEDERAL AVIATION ADMINISTRATION**

1600.60

3/31/80

**SUBJ: PERSONNEL MANAGEMENT INFORMATION SYSTEM (PMIS) SECURITY MANAGEMENT**

1. **PURPOSE.** This order provides guidelines and assigns responsibility for the implementation and administration of a security management program for the Personnel Management Information System.

2. **DISTRIBUTION.** This order is being distributed to the branch level in Washington headquarters, regions, and centers Personnel and Training, Budget, Civil Rights, Management Systems, and Security offices, and the Data Services Division at the Aeronautical Center.

3. **BACKGROUND.**

a. Interest in computer security has escalated over the past several years as a result of the growing concern for individual privacy and the need to protect sensitive data from alteration, destruction, or misuse. Recent legislation and a Government-wide directive published by the Office of Management and Budget (OMB Circular No. A-71) speak to these issues by emphasizing the responsibility of each Federal agency to make certain that appropriate security measures are taken to protect the confidentiality of personnel information and to assure that a sufficient level of security is provided for all data through the use of effective safeguards.

b. The Personnel Management Information System (PMIS) is an integral part of the administrative processes used in the management of agency employees. PMIS contains personnel records on all employees as well as budgeting data relative to authorized and vacant positions. In view of this, it is essential that the availability of the system itself and the accuracy and integrity of the information contained in that system be maintained at the highest level.

4. **SCOPE.** All elements of the Federal Aviation Administration and other agencies under the Department of Transportation who have access to or are involved in the use of the Personnel Management Information System are covered by this order.

5. **PROGRAM OBJECTIVE.** Within the framework of statutory and administrative authority, it is the intent of the FAA to have an effective PMIS computer security management program. This involves the assuring of physical asset protection, accuracy and integrity of data, preservation of personal privacy, and the operational reliability of PMIS. This objective is based upon the recognition that PMIS is an integral part of the administrative

Distribution: A-W(BU/CR/PT/MS/CS)-3; A-XYZ(BU/CR/PM/MS/OS)-3; A-Y(DT)-3

Initiated By: APT-20

page 1

processes used in the management of agency employees and as such is an official source of employee information.

## 6. RESPONSIBILITIES.

a. PMIS system managers serve as the focal point for PMIS activities within their areas of responsibility. As such, they will:

(1) Treat the data contained in PMIS, or that being entered into or extracted from the system, with a degree of sensitivity that will ensure that only those having the right and need to know will have access to the information.

(2) Assign one member to function as a system security officer. In this capacity, the system security officer will be the liaison with the regional security personnel, ensure adherence to accepted physical and operational security standards, and incorporate this aspect of system operations into the region/center evaluation program.

(3) Ensure that all PMIS users are aware that the security, confidentiality, and integrity of the system are fundamentally a user responsibility. As such, system users have a key role to play. Further, users must be made fully cognizant of their responsibilities with respect to data protection and be informed of agency access and disclosure policies and procedures.

(4) Ensure that effective security measures are taken to protect PMIS terminals from physical abuse and to prevent unauthorized access to the system through these terminals.

(5) Develop plans for contingency action to overcome problems resulting from a prolonged system outage.

b. Agency supervisors one level above the system manager, with respect to systems of records over which he or she exercises line supervision, will make appropriate determinations to disclose records or deny requests in accordance with the safeguard requirements contained in Order 1350.22, Protecting Privacy of Information about Individuals and Order 1200.2A, Public Availability of Information. These two orders also point out pertinent civil remedies and criminal penalties for any violations.

c. Personnel Management Information and Analysis Staff (APT-20) exercises national management responsibility for PMIS, and as such serves as the focal point for administration and operation of the system. In this capacity, APT-20 will:

(1) Designate one member to serve as the overall or national system security officer who will focus upon the adequacy of physical and administrative safeguards.

3/31/80

1600.60

(2) Coordinate national security measures with the Office of Civil Aviation Security.

(3) Ensure the appropriate documentation of maintenance processes and processes to access the system as well as to determine the extent of access by PMIS users.

d. Office of Management Systems will be responsible for such computer hardware and software security considerations as:

(1) Ensure that the security responsibilities inherent in the management function for FAA general purpose computer systems are met by the development and implementation of administrative and operational security controls applicable to the use of general purpose computers within the FAA.

(2) Ensure that appropriate computer hardware and software security measures or techniques are considered and used, when applicable, in the acquisition, development, design, and operation of FAA general purpose computer equipments and software systems or applications.

(3) Determine, in cooperation with the supported component, the requirements to utilize communication security techniques or equipments for non-classified information processed by FAA general purpose computer systems.

e. Data Services Division (AAC-300) exercises management responsibility for the host computers and within its area of responsibility will:

(1) Ensure that appropriate security measures are maintained with respect to the technical and physical security of the PMIS operation and equipment.

(2) Coordinate any security measures with the Investigations and Security Division, AAC-90, and appropriate other organizations.

(3) Develop the wherewithal to produce accurate and timely audit trails which would identify who has access to which data within the system.

f. Office of Civil Aviation Security will be responsible for such security measures as:

(1) Conduct security inspection of PMIS facilities on an annual basis reviewing such areas as PMIS record storage practices, FAA Privacy Act record destruction procedures, equipment security, user sensitivity, operational security, etc.

(2) Develop a comprehensive security education program oriented to making PMIS users cognizant of automated system security responsibilities and standards.

(3) Develop, in conjunction with the FAA Safety Engineer, minimum fire protection standards for PMIS terminal cluster rooms.

g. All agency employees having responsibilities for collecting, maintaining, using, disseminating records of identifiable data, or those engaged in the design, development, operation, or maintenance of PMIS records have an ongoing responsibility for adhering to the spirit and intent of FAA rules and regulations and other Governmental directives as well as applicable laws including those dealing with privacy of individuals and freedom of information.

7. SECURITY STANDARDS. System managers, AAC-300, APT-20, and all other appropriate PMIS organizations and personnel will implement procedures to ensure that relevant computer system safeguards are taken. These include physical security measures and operational system security control measures.

a. Physical security deals with securing the physical environment of the terminals, most computers and data storage areas as well as taking measures to prevent or minimize damage as a result of accident, fire, or malicious damage. These include taking such actions as:

(1) Positive personnel access controls will be established to assure that only authorized personnel have access to computer equipment rooms, remote terminal areas, media libraries, and other sensitive areas not within the confines of the central computer facility.

(2) Those areas specified above which are not occupied after or prior to normal duty hours will be secured to prevent or to detect unauthorized entry.

(3) An appropriate combination of physical and procedural controls should be established to protect source materials and input and output documents from theft, loss, or alteration. Computer-generated output containing Privacy Act data shall be safeguarded to prevent unauthorized dissemination or acquisition. The responsibility for protecting this material passes to the user upon delivery or receipt.

(4) The vulnerability of the facility and the records housed within it to damage or destruction from fire, flood, etc., should be considered in establishing a physical security program. A related concern is the existence of well-coordinated and tested plans that will permit continued processing of essential data without unacceptable delays.

b. Operational system controls refer to actions taken to minimize the potential for intentional or accidental compromise of data. Included are such considerations as:

(1) No sensitive data shall be generated for and released to any individual or organization other than designated recipients identified by the office of primary interest.

(2) All special requests for sensitive data must be authorized in writing by the office of primary interest.

3/31/80

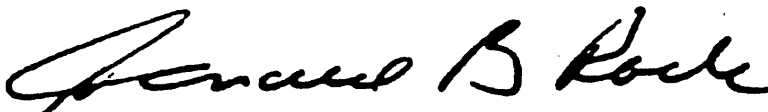
1600.60

(3) All listings, reports, console messages, etc., which remain in the data processing organization and contain sensitive data shall be limited to access on a "need-to-know" basis, and shall be destroyed when no longer needed by shredding, burning, or cutting the printed matter so as to separate the name or identifying number from the data.

(4) Work tapes containing sensitive data shall be controlled until they are scratched, to end of reel, prior to reuse.

(5) All media containing sensitive data shall be controlled during normal duty hours.

(6) Unique user identification password codes shall be maintained in a secure manner and will be limited to bonafide personnel. Employees are to be made aware that password codes are not to be made available to any person or organization other than the one issued the password code.



DONALD B. ROCK  
Director of Personnel and Training

**CHANGE**DEPARTMENT OF TRANSPORTATION  
FEDERAL AVIATION ADMINISTRATION

1600.60 CHG 1

7/17/80

Cancellation  
Date: Retain

SUBJ: PERSONNEL MANAGEMENT INFORMATION SYSTEM (PMIS) SECURITY MANAGEMENT

1. PURPOSE. This change transmits new Appendix 1, Fire Protection Standards for PMIS Terminal Cluster Rooms.2. EXPLANATION OF CHANGE. This appendix prescribes minimum fire protection standards for PMIS cluster rooms where computer terminals, output printers, tape receiving units, supplies, etc., are housed. These standards are applicable to all regions/centers/headquarters where there are such cluster rooms. In nongovernment office space, these standards shall be implemented to the extent consistent with the rental/lease agreements.

## PAGE CONTROL CHART

Remove Pages	Dated	Inserted Pages	Dated
		Appendix 1 Pages 1 and 2	


DONALD B. ROCK  
Director of Personnel  
and TrainingDistribution: A-W(BU/CR/PT/MS/CS)-3; A-XYZ(BU/CR/PM/MS)-3 Initiated By: APT-230  
A-X(CS)-3; A-Z(SE)-3; A-Y(SE/DT)-3

1600.60 CHG 1  
Appendix 1

7/17/80

the transmitting of signals to key personnel in a constantly attended area (e.g., security guard desk) to signify the existence and location of a fire.

c. All smoke detection equipment shall be approved by underwriters laboratories (UL) or Factory Mutual System (FM).

5. EVALUATION PLAN. An emergency evacuation plan shall be developed and personnel in the PMIS room or area made thoroughly aware of the plan. The plan shall include such information as: (a) means of egress from the work area to a designated assembly point outside the building; (b) persons to notify in the event of a fire including the local fire department, security guard, etc.; and (c) procedures to take to minimize fire damage such as closing windows and doors to the work area and disconnecting the electrical power to the ventilation system and equipment in the PMIS room.

6. HOUSEKEEPING. The PMIS terminal room or area shall be kept clean and orderly. Combustible or flammable materials such as paper stock shall not be stored within the terminal room or area.

7/17/80

1600.60 CHG 1  
Appendix 1

the transmitting of signals to key personnel in a constantly attended area (e.g., security guard desk) to signify the existence and location of a fire.

c. All smoke detection equipment shall be approved by underwriters laboratories (UL) or Factory Mutual System (FM).

5. EVALUATION PLAN. An emergency evacuation plan shall be developed and personnel in the PMIS room or area made thoroughly aware of the plan. The plan shall include such information as: (a) means of egress from the work area to a designated assembly point outside the building; (b) persons to notify in the event of a fire including the local fire department, security guard, etc.; and (c) procedures to take to minimize fire damage such as closing windows and doors to the work area and disconnecting the electrical power to the ventilation system and equipment in the PMIS room.

6. HOUSEKEEPING. The PMIS terminal room or area shall be kept clean and orderly. Combustible or flammable materials such as paper stock shall not be stored within the terminal room or area.



**CHANGE**
**DEPARTMENT OF TRANSPORTATION  
FEDERAL AVIATION ADMINISTRATION**

1600.60 CHG 2

**LIBRARY**

3/20/81

 Cancellation  
Date:

**SUBJ: PERSONNEL MANAGEMENT INFORMATION SYSTEM (PMIS) SECURITY MANAGEMENT**

1. **PURPOSE.** This change transmits a revised page to Appendix 1, Fire Protection Standards for PMIS Terminal Cluster Rooms.

2. **EXPLANATION OF CHANGE.** Order 1600.54, Security of FAA Automatic Data Processing Systems and Facilities, states that carbon dioxide or Halon fire extinguishers shall be used on electrical fires. With this change, Order 1600.60 requires that as a minimum, carbon dioxide extinguishers shall be used on electrical fires. This change brings Order 1600.60 in line with Order 1600.54.

**PAGE CONTROL CHART**

Remove Pages	Dated	Insert Pages	Dated
APPENDIX 1 1 and 2	7/17/80	APPENDIX 1 1 2	3/20/81 7/17/80

*Donald B. Rock*  
Donald B. Rock  
Director of Personnel  
and Training

Distribution: A-W(BU/CR/PT/MS/CS)-3; A-XYZ(BU/CR/PM/MS)-3 Initiated By: APT-230  
A-X(CS)-3; A-Z(SE)-3; A-Y(SE/DT)-3

**CHANGE****DEPARTMENT OF TRANSPORTATION  
FEDERAL AVIATION ADMINISTRATION**

1600.60 CHG 1

7/17/80

Cancellation  
Date: Retain**SUBJ: PERSONNEL MANAGEMENT INFORMATION SYSTEM (PMIS) SECURITY MANAGEMENT**

1. **PURPOSE.** This change transmits new Appendix 1, Fire Protection Standards for PMIS Terminal Cluster Rooms.

2. **EXPLANATION OF CHANGE.** This appendix prescribes minimum fire protection standards for PMIS cluster rooms where computer terminals, output printers, tape receiving units, supplies, etc., are housed. These standards are applicable to all regions/centers/headquarters where there are such cluster rooms. In nongovernment office space, these standards shall be implemented to the extent consistent with the rental/lease agreements.

**PAGE CONTROL CHART**

Remove Pages	Dated	Inserted Pages	Dated
		Appendix 1 Pages 1 and 2	



DONALD B. ROCK  
Director of Personnel  
and Training

Distribution: A-W(BU/CR/PT/MS/CS)-3; A-XYZ(BU/CR/PM/MS)-3 Initiated By: APT-230  
A-X(CS)-3; A-Z(SE)-3; A-Y(SE/DT)-3

**CHANGE****DEPARTMENT OF TRANSPORTATION  
FEDERAL AVIATION ADMINISTRATION**

1600.60 CHG 2

**LIBRARY**

3/20/81

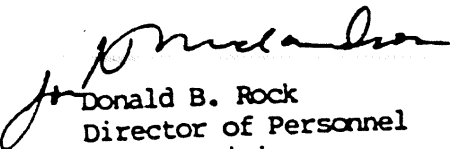
Cancellation  
Date:**SUBJ: PERSONNEL MANAGEMENT INFORMATION SYSTEM (PMIS) SECURITY MANAGEMENT**

1. PURPOSE. This change transmits a revised page to Appendix 1, Fire Protection Standards for PMIS Terminal Cluster Rooms.

2. EXPLANATION OF CHANGE. Order 1600.54, Security of FAA Automatic Data Processing Systems and Facilities, states that carbon dioxide or Halon fire extinguishers shall be used on electrical fires. With this change, Order 1600.60 requires that as a minimum, carbon dioxide extinguishers shall be used on electrical fires. This change brings Order 1600.60 in line with Order 1600.54.

**PAGE CONTROL CHART**

Remove Pages	Dated	Insert Pages	Dated
APPENDIX 1	7/17/80	APPENDIX 1	3/20/81
1 and 2		1	7/17/80
		2	

  
Donald B. Rock  
Director of Personnel  
and Training

Distribution: A-W(BU/CR/PT/MS/CS)-3; A-XYZ(BU/CR/FM/MS)-3 Initiated By: APT-230  
A-X(CS)-3; A-Z(SE)-3; A-Y(SE/DT)-3

APPENDIX 1. FIRE PROTECTION STANDARDS FOR PMIS CLUSTER ROOMS

1. FIRE EXTINGUISHERS. Each PMIS terminal room or area shall be provided with suitable portable fire extinguishers. Fire extinguishers suitable for Class A fires (fires in ordinary combustibles such as wood, paper, etc.) and Class C fires (fires involving energized electrical equipment) shall be provided.

- \* a. In each PMIS room or area there shall be located one water-type extinguisher of a 2 1/2 gallon capacity (2A fire extinguishing rating) and one 15 lb. carbon dioxide extinguisher (class C rating) or one Halon equivalent of at least a 15 lb. capacity for use on electrical fires. Each fire extinguisher shall be clearly marked to indicate the suitability of the extinguisher for a particular class of fire. (Note: Water-type extinguishers shall not be used on Class C electrical fires.) \*

b. Each portable fire extinguisher shall be maintained in a fully charged and operable condition, and kept in its designated place at all times when not being used. Extinguishers shall be located where they will be readily accessible and immediately available in the event of fire.

c. Fire extinguishers shall be visually inspected monthly to ensure that they are in their designated places, fully charged and that there is no obvious physical damage. Annually, extinguishers shall be thoroughly examined and/or recharged or repaired to ensure operability and safety.

d. Personnel working within PMIS terminal rooms or areas shall be trained in the proper use and operation of portable fire extinguishers.

2. ELECTRICAL POWER DISCONNECT SWITCH. An electrical disconnect means/switch shall be provided which disconnects the ventilation system serving the PMIS room or area and the power to all electrical equipment in the room except lighting. The disconnect means shall be controlled from a location(s) readily accessible to personnel within the PMIS room or area and shall be located near the exit from the room. This disconnect means shall be in addition to any individual disconnect switches for components of the data processing system or other electrical equipment.

3. EMERGENCY LIGHTING. Where a loss of commercial power would result in insufficient lighting to permit personnel to exit the PMIS room or area safely, emergency lighting shall be provided.

4. SMOKE DETECTION SYSTEM. A smoke detection system shall be provided in the PMIS terminal room or area when and where electrical equipment remains energized and unattended.

a. Products of combustion detectors, generally of the ionization type, shall be provided in terminal rooms.

b. The operation of the smoke detection system shall cause the sounding of adequate warning signals to permit safe evacuation of all personnel and

**ORDER****DEPARTMENT OF TRANSPORTATION  
FEDERAL AVIATION ADMINISTRATION**

1600.60

3/31/80

**SUBJ: PERSONNEL MANAGEMENT INFORMATION SYSTEM (PMIS) SECURITY MANAGEMENT**

1. **PURPOSE.** This order provides guidelines and assigns responsibility for the implementation and administration of a security management program for the Personnel Management Information System.

2. **DISTRIBUTION.** This order is being distributed to the branch level in Washington headquarters, regions, and centers Personnel and Training, Budget, Civil Rights, Management Systems, and Security offices, and the Data Services Division at the Aeronautical Center.

3. **BACKGROUND.**

a. Interest in computer security has escalated over the past several years as a result of the growing concern for individual privacy and the need to protect sensitive data from alteration, destruction, or misuse. Recent legislation and a Government-wide directive published by the Office of Management and Budget (OMB Circular No. A-71) speak to these issues by emphasizing the responsibility of each Federal agency to make certain that appropriate security measures are taken to protect the confidentiality of personnel information and to assure that a sufficient level of security is provided for all data through the use of effective safeguards.

b. The Personnel Management Information System (PMIS) is an integral part of the administrative processes used in the management of agency employees. PMIS contains personnel records on all employees as well as budgeting data relative to authorized and vacant positions. In view of this, it is essential that the availability of the system itself and the accuracy and integrity of the information contained in that system be maintained at the highest level.

4. **SCOPE.** All elements of the Federal Aviation Administration and other agencies under the Department of Transportation who have access to or are involved in the use of the Personnel Management Information System are covered by this order.

5. **PROGRAM OBJECTIVE.** Within the framework of statutory and administrative authority, it is the intent of the FAA to have an effective PMIS computer security management program. This involves the assuring of physical asset protection, accuracy and integrity of data, preservation of personal privacy, and the operational reliability of PMIS. This objective is based upon the recognition that PMIS is an integral part of the administrative

Distribution: A-W(BU/CR/PT/MS/CS)-3; A-XYZ(BU/CR/PM/MS/CS)-3; A-Y(DT)-3

Initiated By: APT-20

page 1

1600.60

3/31/80

processes used in the management of agency employees and as such is an official source of employee information.

#### 6. RESPONSIBILITIES.

a. PMIS system managers serve as the focal point for PMIS activities within their areas of responsibility. As such, they will:

(1) Treat the data contained in PMIS, or that being entered into or extracted from the system, with a degree of sensitivity that will ensure that only those having the right and need to know will have access to the information.

(2) Assign one member to function as a system security officer. In this capacity, the system security officer will be the liaison with the regional security personnel, ensure adherence to accepted physical and operational security standards, and incorporate this aspect of system operations into the region/center evaluation program.

(3) Ensure that all PMIS users are aware that the security, confidentiality, and integrity of the system are fundamentally a user responsibility. As such, system users have a key role to play. Further, users must be made fully cognizant of their responsibilities with respect to data protection and be informed of agency access and disclosure policies and procedures.

(4) Ensure that effective security measures are taken to protect PMIS terminals from physical abuse and to prevent unauthorized access to the system through these terminals.

(5) Develop plans for contingency action to overcome problems resulting from a prolonged system outage.

b. Agency supervisors one level above the system manager, with respect to systems of records over which he or she exercises line supervision, will make appropriate determinations to disclose records or deny requests in accordance with the safeguard requirements contained in Order 1350.22, Protecting Privacy of Information about Individuals and Order 1200.2A, Public Availability of Information. These two orders also point out pertinent civil remedies and criminal penalties for any violations.

c. Personnel Management Information and Analysis Staff (APT-20) exercises national management responsibility for PMIS, and as such serves as the focal point for administration and operation of the system. In this capacity, APT-20 will:

(1) Designate one member to serve as the overall or national system security officer who will focus upon the adequacy of physical and administrative safeguards.

3/31/80

1600.60

(2) Coordinate national security measures with the Office of Civil Aviation Security.

(3) Ensure the appropriate documentation of maintenance processes and processes to access the system as well as to determine the extent of access by PMIS users.

d. Office of Management Systems will be responsible for such computer hardware and software security considerations as:

(1) Ensure that the security responsibilities inherent in the management function for FAA general purpose computer systems are met by the development and implementation of administrative and operational security controls applicable to the use of general purpose computers within the FAA.

(2) Ensure that appropriate computer hardware and software security measures or techniques are considered and used, when applicable, in the acquisition, development, design, and operation of FAA general purpose computer equipments and software systems or applications.

(3) Determine, in cooperation with the supported component, the requirements to utilize communication security techniques or equipments for non-classified information processed by FAA general purpose computer systems.

e. Data Services Division (AAC-300) exercises management responsibility for the host computers and within its area of responsibility will:

(1) Ensure that appropriate security measures are maintained with respect to the technical and physical security of the PMIS operation and equipment.

(2) Coordinate any security measures with the Investigations and Security Division, AAC-90, and appropriate other organizations.

(3) Develop the wherewithal to produce accurate and timely audit trails which would identify who has access to which data within the system.

f. Office of Civil Aviation Security will be responsible for such security measures as:

(1) Conduct security inspection of PMIS facilities on an annual basis reviewing such areas as PMIS record storage practices, FAA Privacy Act record destruction procedures, equipment security, user sensitivity, operational security, etc.

(2) Develop a comprehensive security education program oriented to making PMIS users cognizant of automated system security responsibilities and standards.

(3) Develop, in conjunction with the FAA Safety Engineer, minimum fire protection standards for PMIS terminal cluster rooms.

1600.60

3/31/80

g. All agency employees having responsibilities for collecting, maintaining, using, disseminating records of identifiable data, or those engaged in the design, development, operation, or maintenance of PMIS records have an ongoing responsibility for adhering to the spirit and intent of FAA rules and regulations and other Governmental directives as well as applicable laws including those dealing with privacy of individuals and freedom of information.

7. SECURITY STANDARDS. System managers, AAC-300, APT-20, and all other appropriate PMIS organizations and personnel will implement procedures to ensure that relevant computer system safeguards are taken. These include physical security measures and operational system security control measures.

a. Physical security deals with securing the physical environment of the terminals, most computers and data storage areas as well as taking measures to prevent or minimize damage as a result of accident, fire, or malicious damage. These include taking such actions as:

(1) Positive personnel access controls will be established to assure that only authorized personnel have access to computer equipment rooms, remote terminal areas, media libraries, and other sensitive areas not within the confines of the central computer facility.

(2) Those areas specified above which are not occupied after or prior to normal duty hours will be secured to prevent or to detect unauthorized entry.

(3) An appropriate combination of physical and procedural controls should be established to protect source materials and input and output documents from theft, loss, or alteration. Computer-generated output containing Privacy Act data shall be safeguarded to prevent unauthorized dissemination or acquisition. The responsibility for protecting this material passes to the user upon delivery or receipt.

(4) The vulnerability of the facility and the records housed within it to damage or destruction from fire, flood, etc., should be considered in establishing a physical security program. A related concern is the existence of well-coordinated and tested plans that will permit continued processing of essential data without unacceptable delays.

b. Operational system controls refer to actions taken to minimize the potential for intentional or accidental compromise of data. Included are such considerations as:

(1) No sensitive data shall be generated for and released to any individual or organization other than designated recipients identified by the office of primary interest.

(2) All special requests for sensitive data must be authorized in writing by the office of primary interest.



1600.60

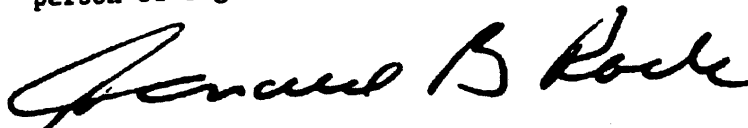
3/31/80

(3) All listings, reports, console messages, etc., which remain in the data processing organization and contain sensitive data shall be limited to access on a "need-to-know" basis, and shall be destroyed when no longer needed by shredding, burning, or cutting the printed matter so as to separate the name or identifying number from the data.

(4) Work tapes containing sensitive data shall be controlled until they are scratched, to end of reel, prior to reuse.

(5) All media containing sensitive data shall be controlled during normal duty hours.

(6) Unique user identification password codes shall be maintained in a secure manner and will be limited to bonafide personnel. Employees are to be made aware that password codes are not to be made available to any person or organization other than the one issued the password code.



DONALD B. ROCK  
Director of Personnel and Training

3/20/81

1600.60 CHG 2  
APPENDIX 1APPENDIX 1. FIRE PROTECTION STANDARDS FOR PMIS CLUSTER ROOMS

1. FIRE EXTINGUISHERS. Each PMIS terminal room or area shall be provided with suitable portable fire extinguishers. Fire extinguishers suitable for Class A fires (fires in ordinary combustibles such as wood, paper, etc.) and Class C fires (fires involving energized electrical equipment) shall be provided.

\* a. In each PMIS room or area there shall be located one water-type extinguisher of a 2 1/2 gallon capacity (2A fire extinguishing rating) and one 15 lb. carbon dioxide extinguisher (class C rating) or one Halon equivalent of at least a 15 lb. capacity for use on electrical fires. Each \* fire extinguisher shall be clearly marked to indicate the suitability of the extinguisher for a particular class of fire. (Note: Water-type extinguishers shall not be used on Class C electrical fires.)

b. Each portable fire extinguisher shall be maintained in a fully charged and operable condition, and kept in its designated place at all times when not being used. Extinguishers shall be located where they will be readily accessible and immediately available in the event of fire.

c. Fire extinguishers shall be visually inspected monthly to ensure that they are in their designated places, fully charged and that there is no obvious physical damage. Annually, extinguishers shall be thoroughly examined and/or recharged or repaired to ensure operability and safety.

d. Personnel working within PMIS terminal rooms or areas shall be trained in the proper use and operation of portable fire extinguishers.

2. ELECTRICAL POWER DISCONNECT SWITCH. An electrical disconnect means/switch shall be provided which disconnects the ventilation system serving the PMIS room or area and the power to all electrical equipment in the room except lighting. The disconnect means shall be controlled from a location(s) readily accessible to personnel within the PMIS room or area and shall be located near the exit from the room. This disconnect means shall be in addition to any individual disconnect switches for components of the data processing system or other electrical equipment.

3. EMERGENCY LIGHTING. Where a loss of commercial power would result in insufficient lighting to permit personnel to exit the PMIS room or area safely, emergency lighting shall be provided.

4. SMOKE DETECTION SYSTEM. A smoke detection system shall be provided in the PMIS terminal room or area when and where electrical equipment remains energized and unattended.

a. Products of combustion detectors, generally of the ionization type, shall be provided in terminal rooms.

b. The operation of the smoke detection system shall cause the sounding of adequate warning signals to permit safe evacuation of all personnel and